GRUPPO DI LAVORO PER LA TUTELA DEI DATI PERSONALI -
ARTICOLO 29

11816/03/FR
WP 86

Documento di lavoro sulle piattaforme informatiche fidate, in particolare per quanto riguarda il lavoro effettuato da Trusted Computing Group (Gruppo TCG)

Adottato il 23 gennaio 2004

Il Gruppo di lavoro è stato istituito a norma dell'articolo 29 della direttiva 95/46/CE. Esso costituisce l'organo consultivo indipendente dell'UE in materia di riservatezza e protezione dei dati. Le funzioni del gruppo sono stabilite dall'articolo 30 della direttiva 95/46/CE e dall'articolo 14 della direttiva 97/66/CE.

Le funzioni di segretariato sono espletate dalla Direzione E (Servizi, proprietà intellettuale e industriale, media e protezione dei dati) della Commissione europea, Direzione generale Mercato interno, B-1049 Bruxelles, Belgio, Ufficio C100-6/136.
Sito web: www.europa.eu.int/comm/privacy

Il GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995[1],

visti gli articoli 29 e 30, paragrafi 1, lettera a, e 3 della suddetta direttiva,

visto il proprio regolamento interno, in particolare gli articoli 12 e 14,

HA ADOTTATO IL SEGUENTE DOCUMENTO DI LAVORO:

Documento di lavoro sulle piattaforme informatiche fidate, in particolare per quanto riguarda il lavoro effettuato da Trusted Computing Group (Gruppo TCG)

Contesto e prospettiva delle piattaforme fidate

Il concetto di piattaforma fidata nasce dalla constatazione dell'industria informatica che l'attuale modello di PC (*Personal Computer*) non è adatto a garantire la sicurezza, come viene dimostrato dagli attacchi di virus, dalla possibilità di spiare i dati che vengono introdotti, dalla pirateria di opere e programmi informatici, ecc.

Tale concetto si sviluppa in un momento in cui si prevede una diminuzione dell'importanza relativa del Web, la parte pubblica di Internet caratterizzata da un numero elevato di transazioni non securizzate, e un aumento degli spazi privati dove la sicurezza sarà una priorità.

Poiché si deve ancora istituire un quadro di sicurezza, la firma elettronica e il suo sviluppo giuridico costituiscono tentativi di risolvere i problemi sollevate dagli scambi in rete; mentre il concetto di piattaforma di fidata mira a fornire una risposta alle questioni connesse alla proprietà, all'integrità, alla riservatezza dei beni intangibili e, all'occorrenza, a controllare il loro impiego in termini di software e hardware. Non tutti i componenti (o building blocks) di queste nuove architetture molto sofisticati sono stati definiti o testati e non tutti sono disponibili. È già noto tuttavia che, a norma dei criteri comuni (*Common Criteria*), tali piattaforme non potranno avere un livello di sicurezza superiore a EAL3, mentre il livello di sicurezza per le carte bancarie con smart chip corrisponde a EAL4 o EAL4+.

I tentativi passati di aumentare la sicurezza individuando i componenti del hardware (ad esempio il Pentium III di Intel che proponeva l'integrazione di un identificatore universale unico) hanno subito una battuta d'arresto a causa dei rischi per la privacy. In seguito a questa esperienza i ricercatori si sono sforzati di conciliare i diversi impieghi delle tecniche sofisticate di codificazione in modo da tutelare la *privacy* ed i dati personali. Per questo motivo le applicazioni di tipo PET (*Privacy Enhancing Technologies*), ad esempio le casseforti digitali individuali ed i sistemi di gestione dell'identità virtuale, sono proposti nell'ambito delle piattaforme fidate. Tuttavia, non è ancora stato prodotto un modello economicamente fattibile di queste funzioni, che sarebbero basate su chip dedicati.

[1] Gazzetta ufficiale n. L 281 del 23/11/1995, pag. 31, disponibile sul sito: http://europa.eu.int/comm/internal_market/privacy/law_fr.htm

Le applicazioni sono pertanto ancora poco sviluppate e l'attenzione s'incentra sulle applicazioni di gestione dei diritti digitali.

Si noti tuttavia che il concetto di proprietà nella società dell'informazione è in piena evoluzione ed è soggetto a controversie accese ma premature. La stabilità giuridica ed economica è ancora lontana. Inoltre, il ruolo svolto dagli spazi pubblici dovrà probabilmente essere riconsiderato.

Il concetto di proprietà fa chiaramente parte delle specifiche per la TCPA (Trusted Computing Platform Alliance) e per il gruppo TCG (Trusted Computing Group), che operano una distinzione netta tra i ruoli di utenti e amministratori. Gli amministratori sono responsabili della definizione e della limitazione dei diritti tecnici e pratici degli utenti e tale situazione solleva ovviamente questioni di equilibrio.

Guardando al futuro i sistemi di gestione dei diritti digitali (DRM- Digital Rights Management) potrebbero essere in grado di definire e securizzare, fino ad un certo punto, l'accesso o l'impiego di dati personali in modo individuale e su base contrattuale. Tali applicazioni non sono mature, perché esistono solo in qualche laboratorio di ricerca e richiedono il supporto di un quadro normativo stabilito. Le piattaforme informatiche in grado di gestire tali diritti saranno le stesse piattaforme fidate oggetto della presente relazione.

Approccio e metodologia del gruppo di lavoro

Il gruppo di lavoro segue con interesse l'evoluzione dell'informatica securizzata, in particolare i lavori effettuati dal Trusted Computing Group (TCG), un consorzio industriale ad hoc che elabora progetti di specifiche per una nuova categoria di chip di sicurezza per il hardware denominata Trusted Platform Module (TPM).

Benché sia consapevole del fatto che il gruppo TCG si concentra essenzialmente sulla definizione di taluni componenti di una piattaforma e non sull'insieme della piattaforma stessa, il gruppo di lavoro riconosce che i componenti (*building blocks*) sviluppati dal TCG (in particolare i TPM) avranno conseguenze importanti per il funzionamento futuro delle piattaforme (PC ma anche computer tascabili (PDA), telefoni mobili, ecc.) operanti in un mondo completamente interconnesso.

La stampa internazionale ha dedicato molta attenzione a quest'evoluzione in seguito alle attività di promozione del gruppo TCG e dei contributi importanti di talune autorità responsabili della tutela dei dati[2] e delle università competenti[3].

Il gruppo di lavoro ha deciso di avviare un dialogo con il gruppo TCG e nel corso del 2003 diverse riunioni sono state tenute tra la Internet Taskforce ed i rappresentanti del gruppo TCG per discutere gli aspetti tecnici e giuridici delle specifiche TCG.
Il gruppo di lavoro constata con piacere che il gruppo TCG ha accolto diversi suoi suggerimenti nella versione 1.2 delle specifiche e ha creato un gruppo di " migliori prassi", che ha il compito di presentare raccomandazioni sulle questioni connesse alla tutela dei dati.
Il presente documento mira a sottolineare alcune delle tematiche che meritano una maggiore attenzione e che dovrebbero essere ulteriormente prese in considerazione dal gruppo TCG.

La valutazione del lavoro del gruppo TCG oggetto del presente documento è limitata dal livello attuale di sviluppo delle specifiche. In questo momento non è ancora possibile sapere come le specifiche saranno utilizzate, quali applicazioni o sistemi operativi saranno sviluppati, quali operatori saranno interessati o quali modelli commerciali saranno sviluppati, ecc. Un altro elemento

[2] Riferimento ai documenti della CNIL, ufficio di Alexander Dix...
[3] Riferimento ai lavori di Ross Anderson.

d'incertezza consiste nel fatto che le specifiche non costituiscono un obbligo a utilizzare tutti i loro elementi né di integrare le nuove caratteristiche di cui alla versione 1.2. Non tutte le funzioni definite nella versione 1.2 delle specifiche TPM saranno applicate in ogni singolo componente della piattaforma.

Di conseguenza saranno necessari ulteriori lavori; il gruppo di lavoro seguirà gli sviluppi, in particolare quelli riguardanti le applicazioni specifiche.

Che cosa è il gruppo TCPA/ TCG?
In base alle dichiarazioni del gruppo stesso la missione del TCG è quella di sviluppare e di promuovere specifiche industriali standard aperte e non legate a un fornitore per i componenti ("building blocks") informatici fidati e per le interfacce di diverse piattaforme. Il TCG è un organismo senza scopi di lucro che raggruppa membri di diversi paesi che hanno adottato come base di partenza le specifiche della TCPA (alleanza per l'informatica fidata).

Al gruppo (un consorzio industriale ad hoc) appartengono molti operatori importanti del settore tecnologico dell'informatica e di altre discipline. È interessante notare, ad esempio, che Sony fa parte di questo gruppo[4].

I Trusted Platform Modules (TPM) basati sulla specifica 1.1b della TCPA sono attualmente disponibili presso tre fornitori: Atmel, Infineon e National Semiconductor. Talune piattaforme microinformatiche sono già commercializzate: i notebook IBM ThinkPad ed i computer da ufficio NetVista. L'industria auspica che altre saranno disponibili in futuro.

Il TCG ha elaborato le specifiche per una nuova categoria di chip di sicurezza (TPM). Questi chip sono destinati all'informatica generale e gli sforzi riguardano essenzialmente la securizzazione delle piattaforme del hardware. Gli obiettivi principali del gruppo TCG sono l'autenticazione e l'aumento del livello di sicurezza. Inoltre, i prodotti TCG consentiranno di realizzare reti informatiche a maglia[5].

I chip TPM comprendono le seguenti funzioni:

- chiave pubblica: generazione di coppie di chiavi, firma per chiave pubblica, verifica, criptaggio e decriptaggio;

- avvio fidato: i registri di configurazione della piattaforma (PCR) registrano hash di informazioni di configurazione in tutta la sequenza di avvio (boot). Una volta avviato il computer, i dati (quali le chiavi simmetriche per i file criptati) possono essere "sigillati" sotto un PCR;

- inizializzazione e gestione: tali funzioni consentono al proprietario di accendere o spegnere le funzioni del chip, di azzerarlo e di prendere il controllo totale ("to take ownership"). La nuova versione delle specifiche consente al proprietario di delegare un certo numero di funzioni all'utente.

---

4 All'inizio, la Trusted Computing Platform Alliance (TCPA) era composta da Compaq, HP, IBM, Intel e Microsoft. Attualmente i promotori del TCG sono AMD, HP, IBM, Intel e Microsoft, ma sono previsti altri promotori. I contribuenti attuali, che comprendono degli europei, sono ATi Technologies, Atmel, Broadcom Corporation, Comodo, Fujitsu Limited, Gemplus, Infineon, Legend Limited Group, National Semiconductor, Nokia, MTRU Cyrptosytems, nVidia, Phoenix, Philips, Rainbow Technologies, Seagate, Shang Hai Wellhope Information, Sony, Standard Microsystems, STMicroelectronics, Texas Instruments, Ultimaco Software AG, VeriSign e Wave Systems. Altre società come Sun Microsystems hanno espresso l'interesse o l'intenzione di entrare nel gruppo.

5 Le reti a maglia consentono la condivisione, la selezione e l'aggregazione di una grande varietà di risorse informatiche ripartite geograficamente (come i supercalcolatori, grappoli di calcolatori, sistemi di stoccaggio, fonti di dati, strumenti, persone) e le presentano come un'unica risorsa.

La tecnologia dei TPM consente l'applicazione di fonti e politiche fidate.

Lo sviluppo di applicazioni specifiche è ancora nella fase iniziale. Taluni esempi di possibili applicazioni sono la gestione dei diritti digitali (DRM)[6], la piattaforma informatica securizzata della nuova generazione (ex-Palladium) di Microsoft e la tecnologia Intel LaGrande. Attualmente non è possibile avere una panoramica completa delle future utilizzazioni delle specifiche TCG.

Come indicato in documenti precedenti relativi a tematiche simili[7], il gruppo di lavoro ribadisce che il gruppo TCG è responsabile almeno dello sviluppo tecnico del progetto. Esso deve inoltre garantire che le specifiche ed i protocolli elaborati consentano agli utenti di conformarsi alle disposizioni della direttiva[8].

Seppure a livelli diversi, sono responsabili della tutela dei dati sia chi realizza le specifiche tecniche sia chi costruisce o sviluppa le applicazioni o i sistemi operativi. Anche chi realizza, commercializza e utilizza le applicazioni ha una responsabilità, in particolare le organizzazioni che trattano i dati degli utenti, poiché sono di norma gli ultimi della catena e quelli che interagiscono con l'utente.

Quadro normativo

Il gruppo di lavoro (articolo 29) ricorda che il lavoro del gruppo TCG dovrebbe tenere conto della legislazione in vigore. Le direttive 95/46/CE e 2002/58/CE sono gli strumenti principali riguardanti la tutela dei dati in generale e dei dati delle comunicazioni elettroniche. In questo contesto si deve tenere conto anche delle disposizioni delle direttive "commercio elettronico"[9] e "firme elettroniche"[10].

Molti principi della direttiva sulla tutela dei dati hanno conseguenze importanti in questo settore. Il gruppo di lavoro desidera sottolineare l'importanza dei principi di proporzionalità e di necessità di raccolta e di trattamento dei dati. In base a tali principi è necessario trovare un equilibrio tra i diritti fondamentali degli interessati e gli interessi dei diversi operatori e limitare al minimo possibile i trattamento di dati personali.
Tali principi incidono sull'elaborazione di nuovi protocolli e dispositivi: benché la tecnologia sia neutra per natura, le applicazioni e l'elaborazione di nuovi strumenti tecnologici dovrebbero sempre rispettare il principio di tutela della sfera privata[11].

Il gruppo di lavoro conosce e sostiene i lavori intrapresi dalla Commissione europea nel settore delle tecnologie di tutela della privacy (*Privacy enhancing technologies)*, e invita il gruppo TCG a continuare ad applicare la filosofia PET ai suoi lavori futuri.

Qualche riflessione riguardante l'incidenza dei lavori del TCG sulla tutela dei dati

---

6 Il gruppo di lavoro effettuerà taluni lavori in questo settore nel prossimo futuro.

7 Si veda, ad esempio, il documento di lavoro sui servizi di autenticazione in linea, adottato il 29 gennaio 2003, WP.

8 Si veda anche la direttiva 99/5 relativa riguardante le apparecchiature radio e le apparecchiature terminali di telecomunicazione e il reciproco riconoscimento della loro conformità, Gazzetta ufficiale L 091 del 07/04/1999.

9 Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (direttiva sul commercio elettronico), Gazzetta ufficiale delle Comunità europee del 17 luglio 2000, L 178/1 à 178/16.

10 Direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche, Gazzetta ufficiale delle Comunità europee, 19 gennaio 2000, L 13/12 à 13/20.

11 Cfr. parere 2/2002 sull'uso di identificativi esclusivi negli apparecchi terminali di telecomunicazione: l'esempio dell'IPv6, adottato il 30 maggio 2002, WP 58

Poiché il quadro tecnologico è ancora in fase di discussione, il gruppo desidera limitarsi ad alcune riflessioni generali sulle linee guida di base utilizzate comunemente dall'industria.

- Ambiente di utilizzazione

Qualsiasi analisi dell'incidenza dei lavori del gruppo TCG sulla tutela dei dati deve distinguere tra i diversi ambienti in cui possono essere utilizzate le piattaforme conformi alle specifiche TCG:
- a livello delle imprese l'infrastruttura proposta potrebbe essere utile per migliorare la sicurezza, in particolare per le reti informatiche. È importante notare che secondo il gruppo TCG le imprese sono i principali consumatori/utenti del sistema;
- a livello dei consumatori è meno chiaro quali siano i vantaggi per l'utente. Il TCG potrebbe fornire alcuni miglioramenti dal punto di vista dell'utente in materia di stoccaggio securizzato e di impiego di pseudonimi digitali per le transazioni. Tuttavia, le applicazioni basate sui TPM potrebbero anche essere utilizzati a scapito degli utenti, ad esempio dall'industria di contenuto al fine di riprendere il controllo della distribuzione e dell'utilizzazione di contenuti digitali (software incluso) che avevano perso con l'arrivo di Internet e delle applicazioni peer-to-peer.

- La libertà di scelta nell'utilizzazione dei TPM

Le specifiche dei TPM distinguono tra il ruolo del proprietario dei diritti e il ruolo dell'utente. Tale distinzione non ha conseguenze per la sfera privata, poiché un individuo sarebbe nel contempo proprietario e utente, ma potrebbe sollevare talune questioni a livello delle imprese.
Nell'impresa il dipendente è l'utente e il datore di lavoro è il proprietario. Il proprietario può prendere una serie di decisioni che riguardano il dipendente e la quantità di dati personali dell'individuo che vengono trattati. In questo caso è responsabilità del proprietario (datore di lavoro) informare l'utente e garantire una tutela adeguata degli individui.

La versione 1.2 delle specifiche ha introdotto alcuni miglioramenti di questa situazione aggiungendo un sistema di delega per le decisioni relativi alle varie funzioni del TPM. Tuttavia, il proprietario dispone sempre del controllo finale e può decidere di delegare o no talune funzioni chiave. In tal caso non è possibile affermare (come fanno talune società TCG sul proprio sito Internet o nelle comunicazioni ufficiali) che gli individui hanno la totale libertà di accettare o no l'impiego del sistema.

In questo momento la possibilità dell'utente di decidere di utilizzare o no una piattaforma con un TPM esiste al di fuori dell'ambiente delle imprese, ma occorre chiedersi per quanto tempo ancora. L'impiego di TPM, incoraggiato da una forte rappresentazione dell'industria potrebbe diventare de facto una norma, una caratteristica necessaria per partecipare alla società dell'informazione. Ciò potrebbe avere conseguenze non solo per la tutela dei dati ma anche per i diritti fondamentali come la libertà d'espressione.

- Informazione degli utenti

In pratica la complessità tecnica dei sistemi basati sui TPM consente difficilmente di supporre che l'utente medio sia in grado di capire le informazioni riguardanti il sistema e di fare scelte informate sul loro uso comprendendo tutte le conseguenze. Il gruppo di lavoro invita il gruppo TCG a garantire che un'informazione semplice e comprensibile sia fornita agli utenti e, ancora più importante, ad assicurare una tutela sufficiente in qualsiasi caso, indipendentemente dalle scelte dell'utente.

- Le caratteristiche della sicurezza

Le specifiche TPM contengono caratteristiche positive per la sicurezza. La sicurezza e l'integrità sono naturalmente aspetti importanti che sono ugualmente pertinenti nel contesto della direttiva sulla tutela dei dati. Il gruppo di lavoro si chiede tuttavia se il livello di sicurezza potrà essere regolato caso per caso in funzione degli impieghi specifici del sistema. La sicurezza dovrebbe, in effetti, essere proporzionale ai rischi, e tali rischi variano a seconda della situazione: ad esempio, se un utente desidera consultare un fascicolo medico in linea il livello di sicurezza richiesto sarà maggiore rispetto a quello necessario nel caso di un individuo che desidera iscriversi ad un sito web che offre un servizio di informazione.

- La tutela dei dati mediante una certificazione esterna o l'anonimizzazione

Per limitare la trasmissione di identificatori e quindi la compilazione da parte di terzi di profili dell'utente, il gruppo TCG prevede la possibilità d'intervento da parte di un terzo fidato che certifica l'identità degli utenti e li conferma al corrispondente senza rivelare l'identità dell'utente.
Il ruolo del terzo fidato (denominato anche "Privacy Certification Authority" dal TCG) deve essere studiato in dettaglio. La concentrazione di dati comporta sempre rischi supplementari e quindi vanno prese le dovute precauzioni. Per quanto riguarda i TPM esistono scenari in cui un unico terzo fidato controlla enormi quantità di informazioni di autenticazione.
La versione 1.2 delle specifiche consente di evitare il terzo fidato mediante l'utilizzo della funzione di "Direct Anonymous Attestation (DAA)", che consente all'utente di creare un "Attestation Identity Key" (AIK- chiave di attestazione dell'identità) senza presentare la chiave di approvazione (Endorsement Key, EK), che è un identificatore unico[12]. Il gruppo di lavoro ritiene che si tratta di un miglioramento, ma sottolinea che la scelta tra terzo fidato e DAA sarà fatto a livello delle applicazioni. Le specifiche attuali permetteranno ancora le due funzioni.

La DAA è quindi una possibilità supplementare ma non una caratteristica standard del sistema. Il gruppo di lavoro ritiene che l'introduzione della funzione DAA[13] costituisca un miglioramento, ma ricorda che non si può più parlare di anonimato[14] quando è possibile creare un legame con l'identità dell'utente o stabilire profili degli utenti Esso invita il gruppo TCG a promuovere l'impiego di tale funzione in modo da tutelare la privacy ed i dati, vale a dire mediante l'utilizzo di identificatori aleatori e limitando l'uso dei nomi al periodo più breve possibile nei casi in cui è necessaria la revoca o l'identificazione.

Il gruppo di lavoro ribadisce l'importanza della fiducia nei sistemi basati sui TPM. La fiducia deve esistere in tutta la catena degli operatori interessati, da chi realizza specifiche, al venditore delle applicazione e all'utente del sistema. È necessario tutelare i dati in tutte le fasi.

Elementi che meritano un'ulteriore considerazione nelle linee guida e migliori prassi che vanno stabilite dal gruppo TCG

Il gruppo di lavoro ritiene che sia utile creare all'interno del gruppo TCG un gruppo "migliori prassi" che tratterà le questioni di tutela dei dati e svilupperà orientamenti e prassi migliori in questo campo.

---

[12] La DAA fornisce un'alternativa al metodo del terzo fidato per stabilire la validità di un AIK. Essa utilizza la tecnica criptografica di "zero knowledge proof" e stabilisce la validità dell'AIK senza svelare i riferimenti dell'EK al fornitore d'identità.

[13] La mancanza di esperienza pratica del funzionamento dei sistemi di controllo a "zero knowledge" rende difficile valutare come la DAA potrebbe funzionare nella prassi.

[14] Cfr. considerando 26 della direttiva sulla tutela dei dati.

Il ruolo di questo gruppo sarà molto importante per garantire un'applicazione delle specifiche del gruppo TCG che rispetti la privacy e le libertà fondamentali. Il gruppo di lavoro invita questo gruppo a trattare i seguenti punti.

- Ruolo dei terzi fidati (Privacy CA): chi saranno i terzi fidati e quale ruolo ricopriranno? Il gruppo "migliori prassi" potrebbe elaborare linee guida sulle misure di salvaguardia necessarie. Il terzo fidato stabilito in Europa deve operare nel rispetto delle norme sulla tutela dei dati e deve tenere conto delle disposizioni delle direttive sul commercio elettronico e sulle firme elettroniche.

- Utilizzo della funzione DAA: il gruppo "migliori prassi" dovrebbe promuovere gli identificatori aleatori come prima scelta, sempre che non sia specificamente necessario utilizzare il nome. Se il nome è necessario, va utilizzato per un periodo breve, in modo da evitare qualsiasi possibilità di stabilire profili dell'utente a lungo termine e, inoltre, deve essere informato l'utente. Il gruppo "migliori prassi" potrebbe elaborare esempi di servizi diversi e indicare il modo in cui la DAA va utilizzata in ogni contesto per illustrare i problemi ed individuare le questioni chiave.

- Informazione degli utenti: le informazioni devono essere complete, facili da comprendere e fornite all'utente a diversi livelli. Esiste una catena di responsabilità che va da chi elabora le specifiche ai produttori, agli addetti allo sviluppo di nuovi sistemi operativi o applicazioni, a chi li commercializza, ecc. L'impiego dei TPM deve essere trasparente per l'utente, in particolare a livello dell'applicazione.
Il gruppo di lavoro deplora il fatto che la complessità tecnica dei sistemi basati sui TPM comporti per l'utente medio grandi difficoltà di comprensione delle cause e delle conseguenze dell'utilizzazione di talune caratteristiche del sistema e invita il gruppo TCG a produrre fascicoli di informazione in un linguaggio chiaro e semplice che consenta all'utente di comprendere la tecnologia e le responsabilità.

- Necessità di controllo e miglioramento: il gruppo di lavoro è consapevole del fatto che il gruppo TCG non può controllare completamente la conformità delle applicazioni in materia di tutela della privacy, ma ritiene che sarebbe utile introdurre nei sistemi taluni meccanismi di controllo dell'applicazione delle specifiche. La creazione di un logo o di un programma di certificazione riguardante la conformità dei prodotti è stata proposta nel corso del dialogo con i membri del gruppo TCG.
Il gruppo di lavoro desidera incoraggiare il gruppo TCG a studiare tali possibilità e ad elaborare raccomandazioni e linee guida che motivano le imprese a utilizzare le specifiche in modo da rispettare o perfino migliorare la tutela della privacy e delle libertà fondamentali. Una particolare attenzione va accordata al contributo specifico della legislazione europea in questo campo.

Conclusione

Il gruppo di lavoro constata con soddisfazione che il gruppo TCG ha accolto diverse sue proposte nella versione 1.2 delle specifiche e ha creato un gruppo "migliori prassi" incaricato di elaborare raccomandazioni sulle questioni connesse alla tutela dei dati, della privacy e delle libertà fondamentali. Esso invita il gruppo TCG a riflettere sulle questioni sollevate nel presente documento e ad inserire nel sistema caratteristiche che rispettano la sfera privata e migliorano la tutela della privacy.

Finora le specifiche del gruppo TCG praticamente non sono state utilizzate e in futuro potrebbero essere modificate. Talune delle possibili utilizzazioni di questa tecnologia non sono ancora state individuate e numerose questioni saranno decise a livello delle applicazioni. Nuove funzioni vanno

inserite in piattaforme diverse dal PC, ad esempio telefonia mobile, PDA, ecc. Esiste pertanto una grande incertezza a livello dei servizi e delle applicazioni.

Il gruppo di lavoro continuerà pertanto a seguire gli sviluppi al fine di garantire il rispetto delle disposizioni della direttiva. Esso invita il gruppo TCG a presentare periodicamente relazioni al gruppo di lavoro sui progressi e sullo sviluppo delle applicazioni e, in particolare, sui lavori del gruppo "migliori prassi" e del gruppo dei consulenti.

Fatto a Bruxelles, il 23 gennaio 2004
Per il gruppo di lavoro
Il Presidente
Stefano RODOTA